

# TÍTULO DE LA TAREA



## Índice

Enunciado de la tarea.....	3
Introducción.....	4
Parte 2.....	4
Noticia 1.....	4
Noticia 2.....	4
Noticia 3.....	4

# Enunciado de la tarea

## **Tarea: Ampliación de amenazas y análisis de ataques al Internet de las Cosas (IoT)**

### Parte 2: Investigación de ataques al Internet de las Cosas (IoT)

Realiza una investigación sobre ataques recientes a dispositivos del Internet de las Cosas (IoT). Encuentra noticias actuales que detallen incidentes de seguridad, brechas de privacidad o vulnerabilidades en dispositivos conectados como cámaras de seguridad, electrodomésticos inteligentes, automóviles conectados, etc.

- Noticias y análisis: Describe los ataques más recientes, explica sus causas y consecuencias, y cómo afectan la seguridad del IoT.

Presentación en clase:

# Introducción

Los IoT (Internet de las cosas), es una característica, de los dispositivos, los cuáles se comunican a Internet, pueden ser desde la domótica en una casa, un Walkie-Talkie, un teléfono móvil.

## Parte 2

### Noticia 1

Descubren una variante del gusano RapperBot, que infecta dispositivos IoT para lanzar ataques DdoS

La primera vez que se lanzó un ataque con este “gusano”, fue en 2022, teniendo como objetivo el protocolo SSH; este gusano, se llama Mirai, y hace un ataque de fuerza bruta, de manera inteligente. Éste comprueba el prompt para poder usar las credenciales adecuadas de manera adecuada.

Más información [aquí](#).

### Noticia 2

La nueva botnet de IoT "Raptor Train" compromete más de 200.000 dispositivos en todo el mundo

Un grupo de amenazas con sede en Pekín llamado Integrity Technology Group ha creado una botnet que ha infectado a más de 260000 dispositivos, de todo tipo, desde cámaras IP, enrutadores, NAS, etc.

Este año el FIB ha conseguido desmantelar la botnet en 2024.

Para saber más pincha [aquí](#).

### Noticia 3

Alertan de un nuevo método para robar autos con un truco de IoT

Un hombre ha descubierto recientemente en Londres que el parachoques delantero y el faro izquierdo de su Toyota RAV4 habían sido golpeados mientras estaba estacionado. El enchufe del cableado del faro había sido arrancado, y había marcas de destornillador, por lo que concluyó que no había sido un accidente. La situación volvió a repetirse un mes después, pero el dueño del vehículo no cayó en la cuenta de que se trataba de un sabotaje hasta que su Toyota desapareció, mientras que en la aplicación móvil del coche veía que su vehículo estaba en movimiento.

Noticia completa [aquí](#).

## Noticia 4

### Expuestos los datos de 850.000 clientes de Iberdrola

Iberdrola sufrió un ataque que afectó a más de 850000 clientes en mayo de 2024; no afectó a los datos financieros del usuario, pero sí a su nombre y DNI. Tuvo lugar entre el 5 y el 7 de mayo. Llegó a través de un proveedor, esta empresa tiene más de 11 millones de usuarios, lo cuál habría podido ser una catástrofe inmensamente más grande de lo que fue.

Más información [aquí](#).